The Effect of Threat and Proximity on Cyber-Rumor Sharing

Rohit Valecha[1(✉)], Tejaswi Volety[1], K. Hazel Kwon[2], and H. Raghav Rao[1]

[1] University of Texas at San Antonio, San Antonio, TX 78249, USA
{rohit.valecha,hr.rao}@utsa.edu,
teja.volety@gmail.com
[2] Arizona State University, Phoenix, AZ 85004, USA
khkwon@asu.edu

Abstract. Today's society faces a paramount challenge from cyber-rumors that become rapidly viral and transform into more harmful impacts in social networks. The problem of cyber-rumors is further exacerbated in the health crisis context. In the healthcare literature, it has been well established that threat situations facilitate citizens' behavior including cyber-rumor sharing. In this paper, we argue that in the healthcare context, both the threat attribute and cyber-rumor sharing are likely to be influenced by the proximity to health crisis. We argue that proximity is an important indicator of newsworthiness and shareworthiness in social media. In accordance, we investigate how the concept of proximity affects diffusion characteristics of cyber-rumor messages. We address the following research questions associated with cyber-rumor sharing in the context of Zika virus: How does proximity affect the threat appeal in a cyber-rumor message? How does proximity influence cyber-rumor sharing? The results indicate the negative effect of spatial and temporal distance on threat appeal, and the negative effect of spatial distance on cyber-rumor sharing. Such an investigation allows us to quickly identify the emergence of viral rumor messages and monitor the ongoing development of these messages in a timely manner.

Keywords: Rumor · Cyber-rumor sharing · Threat · Proximity

1 Introduction

Today's information and communication technologies (ICTs) faces a big challenge from cyber-rumors (Oh et al. 2013; Rao 2016). Cyber-rumors can become rapidly viral and transform into more harmful impacts in social networks (Webb et al. 2016). The problem of cyber-rumors in the health crisis context is further exacerbated due to the following reasons: The health sector cannot rely on public opinion to infer true information. In fact, much of the population is inadequately equipped to evaluate health-related information provided on the social media and healthcare communities. Reliable information from reputable sources such as medical journals, medical societies, WHO, CDC, etc. takes a significant time delay. These delays encourage health-related cyber-rumors. The more citizens accept health-related cyber-rumors, the greater

S. K. Sahay et al. (Eds.): SKM 2019, CCIS 1186, pp. 182–193, 2020.
https://doi.org/10.1007/978-981-15-3817-9_11

is the misunderstanding between healthcare experts and civil society, which can weaken the effectiveness of health crisis response (Valecha et al. 2017). This is the reason why, The Atlantic stated, "of all the categories of [misinformation], health news is the worst."[1]

A key element for successful health-related cyber-rumor management is "to understand what makes citizens prone to engaging in [health-related] cyber-rumor sharing" (Kwon and Rao 2017; p. 307). In the healthcare literature (though not related to cyber-space), it has been well established that threat situations facilitate citizens' behavior (Folkman 2013; Rogers 1975; Witte 1992). Prior literature in the rumor context has investigated the effect of threat on cyber-rumor sharing (Kwon and Rao 2017). It has found that threat increases the willingness of cyber-rumor sharing. In this paper, we define threat appeal as a persuasive message that attempts to arouse fear through the threat of impending danger or harm. We argue that, in the healthcare context, both the threat appeal of a cyber-rumor message and cyber-rumor sharing are likely to be influenced by the proximity to health crisis. Proximity has been considered as an important indicator of newsworthiness (Nossek and Berkowitz 2006) and "shareworthiness" in social media (Trilling et al. 2017). We investigate how the concept of proximity affects diffusion characteristics of cyber-rumor messages.

Based on the discussion by Trope and Libermann (2010), we utilize social, temporal and spatial distances (also referred to as psychological distances) to elaborate the notion of proximity in a generalizable and operational way, and address the following research questions associated with cyber-rumor sharing in the context of Zika virus: How does psychological distance affect the threat appeal in a cyber-rumor message? How does psychological distance influence cyber-rumor sharing? In order to address these research questions, using Twitter data, we investigate the effect of social, temporal and spatial distances on cyber-rumor sharing. The results indicate that spatial and temporal distance have a negative effect on threat appeal, while spatial distance has a negative influence on cyber-rumor sharing.

Such an investigation will allow us to quickly identify the emergence of viral rumor messages and monitor the ongoing development of these messages in a timely manner. It will also allow practitioners and policymakers flag and correct highly threatening messages in the proximity of the event and location to reduce chaos and uncertainty related to the event. It will allow more efficient utilization of communication channels in order to help healthcare officials to reduce panic situations and promote reliable information sharing (Volety et al. 2018). This research is a step towards "bright ICTs" that counter the negative effects of technologies and help establish a safe and secure society (Lee 2015, 2016). The rest of the paper is organized as follows: First we discuss the literature on cyber-rumor sharing as well as shed light on the theoretical lens. Then we discuss the methodology consisting of data collection, unsupervised machine learning and quantitative analysis. After discussing the results in the subsequent section, we conclude with future work for completing this research.

[1] https://www.theatlantic.com/health/archive/2017/06/of-all-the-categories-of-fake-news-health-news-is-the-worst/531540/.

2 Theoretical Background

2.1 Crisis Situation, Threat Appeal and Cyber-Rumor Sharing

People have started relying heavily on social media for any news updates (Valecha et al. 2010). Owing to the outpour of social media information from various user groups coupled with its unstructured nature, there is a high probability of false information being spread or the information getting manipulated through various discussions (Oh et al. 2013). There are numerous studies that have investigated diffusion characteristics and other metadata related properties around a message and the network from which the message is initiated (Li et al. 2014; Suh et al. 2010). Studies have also compared diffusion for non-rumor, rumor, and rumor-correcting messages (Lee et al. 2015; Shin et al. 2012).

Rumors diffuse even more readily under the crisis context that invokes a sense of fear in public minds (Pezzo and Beckstead 2006). In the context of Zika virus, a possibility of newborn's brain defect without a known treatment induces a high level of anxiety and uncertainty, the two prerequisites of threat situation (Oh et al. 2013), especially among pregnant women. Under such a threat situation, individuals will engage in various social behaviors that help reduce fear, such as religious activities (Solomon et al. 1991). Cyber-rumor sharing is one way to collectively manage fear associated with the threat situation (Kwon and Rao 2017). That is, the threat situation serves as an important antecedent of cyber-rumor sharing; it increases the willingness of cyber-rumor sharing. Nonetheless, as Kwon and Rao (2017) pointed out, "studies that investigate the threat situational effect in the real-world context are very rare" (p. 309).

In the context of social media messages, a message can depict threat in a certain way to invoke a sense of fear. We conceptualize a message's threat appeal as a persuasive attempt to arouse fear through the threat of impending danger or harm. The effect of threat appeal has been attested in cyber-rumoring contexts. For example, Valecha et al. (2017) have shown that threat appeals induced from a rumor message can influence citizens' cyber-rumor sharing. Kwon and Rao's (2017) study has also shown that anxiety aroused by different rumor topics can explain largest variances for citizens' willingness for rumor sharing. While prior literature has focused on the effect of threat appeal on cyber-rumor sharing, however, very few studies have investigated how attributes of a message shape threat appeal within the cyber-rumor messages.

2.2 Psychological Distance and Cyber-Rumor Sharing

Prior studies have contended that tie strength with a message sender influences perceived trustworthiness of rumors, which then influences rumor acceptance and transmission (Oh et al. 2013). Network analysis in the context of rumor diffusion has shown that social network ties and community structures are associated with ways in which rumors are spread (Ye et al. 2018). For example, Cheng et al. (2013) state that closer the ties are the more the message gets spread because it makes the rumor appear to be trustworthy. Similarly, Shin et al. (2012) demonstrate that believers of political rumors formed a more ideologically cohesive, denser community in Twitter than those who refuted rumors.

Tie strength is a way to measure interpersonal affinity (Marsden and Campbell 1984). Trope and Libermann (2010) have defined interpersonal affinity as social distance. While rumors studies have attested to social distance effects on rumor diffusion, little research has paid attention to other factors that together define an individual's overall state of psychological distance. Specifically, psychological distance is a composite construct of three distance variables including social distance, spatial distance and temporal distances (Trope and Liberman 2010). In Twitter context, Kwon et al. (2017) have defined social distance as the measure of how close a user perceives another person—who may be either a message sender or mentioned in the message—as a part of one's social life; spatial distance as the geometric distance of a message receiver from the place where the event occurs; and temporal distance as the distance measured in terms of the time gap between the occurrence of an event and the exposure to message. These three distance variables affect one's psychological distance, which may influence the diffusion of rumor messages.

3 Research Model

As the literature review above suggests, a message invoking a sense of threat/anxiety could increase online public's likelihood of engaging in cyber-rumor sharing. While previous studies on cyber-rumors were done in the contexts of security, politics, and financial crisis (e.g., Kwon and Rao 2017; Oh et al. 2013; Shin et al. 2017), threat appeal could be especially important to explain cyber-rumor sharing in a public health context such as Zika virus because consequences nuanced by the threat appeal could pose immediate relevance to one's personal health risk (Liberman and Chaiken 1991). Based on this rationale, we first examine the effect of rumor message's threat appeal on cyber-rumor sharing.

H1: Cyber-rumor sharing will be positively influenced by threat appeal in a rumor message

Social, spatial and temporal distance are the sub-units (or dimensions) of psychological distance, which may affect one's susceptibility to cyber-rumor message and its diffusion. We argue that the effects of psychological distance on cyber-rumor sharing may be a two-stage process. First, users who feel psychologically close to the Zika Virus issue may feel a greater sense of anxiety. To reduce such anxiety, users may be prone to engaging in conversations directly related to the threat appeal itself. Conversely, users who perceive the issue as a distant event will be less likely to engage with threat appeals. Based on this logic, we post following hypothesis.

H2: Psychological distance, (a) social, (b) spatial, and (c) temporal, will be negatively associated with the presence of threat appeal in a rumor message

Second, psychological distance will affect not only the threat appeal in rumor messages but also the likelihood of it being shared. For example, if a person claimed to be a witness to an event, users in the same social circle or who share similar social identity with the witness would be prone to believing the claim and sharing with their own social circle. Also, a message created from a location closer to where the event occurred would increase its "shareworthiness" (Trilling et al. 2017). Similarly, during the time when an event is rampant, there is a higher probability of a cyber-rumor message being shared (Takayasu et al. 2015) as compared to later in time. This is referred to as the hot topic or trending topic effect that involves connection to time. Accordingly, we argue that, if a cyber-rumor message is closer in social, spatial and temporal distance, there is a high probability that the rumor gets shared.

H3: Cyber-rumor sharing will be inversely influenced by psychological distance, (a) social, (b) spatial, and (c) temporal

Studies have also shown that there are other factors that also have an impact on information sharing behavior in social media, such as hashtags and followers (Stieglitz and Dang-Xuan 2013). We include these variables as controls in the model (Fig. 1).

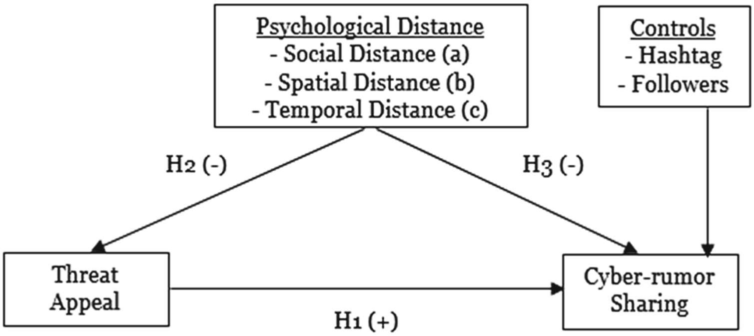

Fig. 1. Research model

4 Methodology

To address our research questions, we developed an approach that streamlines the (iterative) process of data acquisition, data cleansing, and data visualization.

4.1 Data Collection

In this paper, we collected data for Zika outbreak from Twitter about the epidemic by recording the date, content, user, retweet count, Follower count, URL of web content, location from September 2015 to May 2017. Twitter provides three APIs to enable researchers and developers to collect data, namely STREAMING, REST and SEARCH APIs. Satisfying user specified filtering criteria (based on keywords, location, language, etc.), STREAMING API is used to get tweets and their corresponding user's data in real time, REST API is used to get the data in select historical time period, and SEARCH API provides data on relevant searches on Twitter (Valecha et al. 2016). We collected 155,589 tweets by searching data for #zika, #zikavirus and other Zika related hashtags. The tweets were then cleaned, lemmatized and stemmed. This ensured that there are no special characters except line break tweets within the list of sentences. Then we collected known Zika Virus rumors from various sources.

Known rumors in the context of Zika virus were obtained from:

- https://www.nytimes.com/interactive/2016/02/18/health/what-causes-zika-virus-theories-rumors.html?mcubz=0
- https://www.elsevier.com/about/press-releases/research-and-journals/zika-conspiracy-theories-on-social-media-putting-vulnerable-people-at-risk
- https://undark.org/2016/06/01/zika-conspiracy-theories-twitter/
- http://www.snopes.com/americans-immune-zika-virus/

These known rumors were identified as follows:

a) Genetically modified mosquitoes are the real cause of the birth defects
b) Larvicide in drinking water causes microcephaly (Zika virus symptom)
c) Rumors have blamed both a “bad batch of rubella vaccine” and the introduction of a new pertussis vaccine in Brazil, or aluminum in that vaccine
d) Brazil has been undercounting Microcephaly (A symptom where baby's head is significantly smaller than expected, could be due to Zika)
e) Most pregnant women who have Zika have normal babies
f) Microcephaly is caused by the MMR vaccine and pharmaceutical companies are blaming Zika virus in order to profit from selling Zika vaccines.
g) Americans are immune to the Zika virus

From this corpus of Twitter data, we extracted 45,500 unique English tweets related to known rumors in the Zika context. We encountered these rumors from December 2015 to February 2017. We utilized Jaccard matching for matching the tweets with known rumors.

4.2 Measurement

For the dependent variable, cyber rumor-sharing, we chose retweet count that denotes the number of times the rumor tweet has been shared. The control variables, hashtag and followers, were measured as the number of hashtags present in the rumor message, and the natural log of the number of followers of the Twitter user respectively. We chose to use natural log transformation for the follower variable because the followers for some users can be in magnitudes of 10^4 or more. Natural log transformation allows rescaling of the follower variable to be comparable with other variables.

For coding the threat appeal, we utilized content of the tweet. We resorted to unsupervised machine learning using Neural Networks. Our aim was to find the keywords used in similar context as threat within the rumor tweets. This was accomplished in 3 steps: (1) From the 45,500 extracted rumor tweet samples, we created a dataset. (2) We cleaned, lemmatized and stemmed the rumored tweets. (3) We trained a Word2Vec model to identify similar words in a text (where similarity is based on the distance between the keywords).

Word2Vec is a neural network-based algorithm (Goldberg and Levy 2014) that takes words as inputs by converting the words into word embedding. It is an unsupervised machine learning model that does not require any labels and can learn the weights of words as word vector representations incorporating most of the semantically rich information. These vectors can then be used to find similarities between words to get relations. In this study, GenSim Word2Vec model, a Python-based content analysis program, was employed for the analysis of text. Word2Vec model utilized skip-gram algorithm, which predictively learnt the word embedding or the numeric vector representation of words. The algorithm was trained with a window of 4, i.e. the context spans over to at max 4 words to the left and 4 words to the right of the target word, during training. Dimensionality of the feature vectors was set to 45,500, with negative sampling (noise words) was set to 10, to prevent over fitting and increase accuracy, of the learned vectors. The model was trained for 50 epochs.

This trained neural network model understood the context of each word in the dataset, which was then utilized to find specific words indicative of the threat, for example "vector, bacteriophage, virus, arbovirus." The output of the neural network was used as the input for quantitative content analysis.

For coding social distance, we borrowed from Snefjella and Kuperman (2015). They have identified words that are used in similar context as the words that quantify social distance – the degree of willingness to establish some kith with representatives of a social group. The classification identifies acquaintance as the individual's acceptance to a social group using words like "mother, baby, child, family, father, friend" to denote lower social distance, and words such as "neighbor, peer, colleague, mate, tourist, people" to denote higher social distance. For example, the tweet "… experience in brazil zika funding is tremendous victory for sfl grateful to work colleagues who care about our community as it battles the virus" was coded as higher social distance since it refers to the community. These words were used as the input for quantitative content analysis. For quantitative content analysis, the frequency of occurrence for each keyword was used as an indicator of the importance or emphasis, referred to as a "hit". We used the number of hits per rumor tweet and the total number of words contained in that rumor tweet to calculate "hit-density," which represents how densely the keywords are populated in the rumor tweet (Kim et al. 2005; Park et al. 2007). Finally, we dichotomize hit-density to denote the presence or absence of threat within the rumor tweet.

Temporal distance was measured as the natural log of the number of hours between the tweet posting date and the event's peak time, where the peak time quantifies the time of the most influential tweet in that event. Here we assume that tweet peaks denote an important event in that period.

Spatial distance was measured as the natural log of the geographical distance from Brazil – the locus of Zika-related scare. For this purpose, the combination of latitude and longitude of the tweet was used to calculate the distance from Brazil. For example, the tweet "the zika crisis's second wave some babies with zika infection develop microcephaly months after" was reported with location 42.631°, −71.147°. This was compared with location of Brazil 14.235°, 51.925° using Google Distance Matrix API[2] to calculate the distance of 4290 miles.

4.3 Descriptive Statistics

The Spearman rank correlation test (Table 1) indicates that all correlations are less than 0.6, indicating that no significant multi-collinearity problems exist (Kishore et al. 2004). Spearman's coefficient is appropriate for both continuous and discrete ordinal variables. Both Spearman's ρ and Kendall's τ can be formulated as special cases of a more general correlation coefficient. The sample size is large enough to suppress the potential Type I and Type II errors. The concern of Type II errors can be suppressed with a large sample size, and the immunity of Type I error can be ensured by the significance of p-value (Larson-Hall 2010).

Table 1. Correlation results

	1	2	3	4	5	6
1	1					
2	0.598***	1				
3	−0.299***	−0.347***	1			
4	0.045***	0.057***	−0.010*	1		
5	0.098***	−0.492***	0.590***	−0.007	1	
6	−0.042***	−0.159***	0.019***	−0.077***	0.059***	1

* $p < 0.05$; ** $p < 0.01$, *** $p < 0.001$

Legend: (1) Followers, (2) Hashtags, (3) Ln (Spatial Distance), (4) Ln (Temporal Distance), (5) Social Distance and (6) Threat Appeal

4.4 Analysis

In order to examine the hypotheses, we utilized path analysis. Path analysis is suitable for simultaneous equation models. PLS analysis was conducted on the dataset using MPlus tool. The endogeneous variables in the model, retweet is a count variable while threat appeal is a binary variable. This leads to violation of normality in residuals. As a result, Ordinary Least Square (OLS) regression cannot estimate the appropriate statistics. Negative binomial regression has been suggested as a possible method to deal with count endogeneous variables (Osgood 2000), and logistic regression has been suggested for dealing with binary endogeneous variables. In line with this, we specified the cyber-rumor sharing as a count variable and threat appeal as a categorical variable in MPlus. This allows MPlus to model the effect of social, spatial and temporal distances, as well as threat appeal on cyber-rumor sharing (retweet) using negative binomial regression. In addition, based on the specification, MPlus models the effect of

[2] https://developers.google.com/maps/documentation/distance-matrix/intro.

social, spatial and temporal distances on threat appeal using logistic regression. Both logistic and negative binomial regression allow for log likelihood parameter estimation.

5 Results

The results of the analysis are summarized in Table 2. First of all, as hypothesized, spatial and temporal distances are negatively associated with threat appeal at $p < 0.01$ and $p < 0.001$ respectively. This implies that cyber-rumors that are spatially and temporally close to Zika crisis report higher level of threat appeal, supporting H2b and H2c. Contrary to our expectation, social distance is positively associated with threat appeal, opposite to H2a. Further, the results show that the negative effect of spatial distances is significant at $p < 0.001$, implying that closer the spatial distance from the Zika crisis epicenter, greater the likelihood of cyber-rumor sharing. H3b is supported. However, the effect of social and temporal distance on cyber-rumor sharing is positive, contrary to H3a and H3c. We also find opposite effect (i.e. negative) of threat appeal on cyber-rumor sharing. So H1 is not supported.

Table 2. Results of path analysis

	Coefficient	Std. Error	Odds	Support
Effect on threat appeal				
Social distance	0.275***	0.022	1.317	H2a not supported
Ln (spatial distance)	−0.036**	0.012	0.965	H2b supported
Ln (temporal distance)	−0.141***	0.009	0.898	H2c supported
Effect on retweet				
Hashtag	0.426***	0.004	1.531	
Followers	0.007***	0.001	1.007	
Social distance	0.003	0.054	1.003	H3a not supported
Ln (spatial distance)	−0.164***	0.021	0.849	H3b supported
Ln (temporal distance)	0.018	0.023	1.018	H3c not supported
Threat appeal	−0.308***	0.056	0.735	H1 not supported

* $p < 0.05$; ** $p < 0.01$, *** $p < 0.001$

6 Discussion and Conclusion

We examined the effect of social, spatial and temporal distances on threat appeal and sharing of a cyber-rumor message in the Zika Virus context. We analyzed Twitter data generated within the time span of September 2015 to May 2017. The results indicate that spatial and temporal distance is negatively associated with threat appeal. This needs contextual interpretation from the view of "proximity to threat" as follows: Cyber-rumor messages coming from close to Brazil and around important Zika-related events report higher levels of threat appeal associated with the pandemic. Another interesting finding is that spatial distance is negatively associated with the likelihood of cyber-rumor sharing. From the contextual viewpoint, this denotes that cyber-rumor messages coming from close to Brazil spread more.

One reason for the positive effect of social distance on threat appeal is that the group associated with the higher social distance can consist of a larger population (such as neighbors, tourists, etc.) than the group associated with lower social distance. It may provoke large-scale panic due to the collective stress reaction about immediately threatening circumstances to large populations (Oh et al. 2013). Furthermore, the positive effect of temporal distance on cyber-rumor sharing can be explained as the exposure effect – the amount of time the cyber-rumor message is exposed; if the message is exposed for a longer while, it can have more opportunity to accumulate more retweets.

In terms of practical implications, findings of this study can offer directions to practitioners and policy makers to promote mitigation of cyber-rumor messages in the aftermath of health crisis incidents (Valecha et al. 2017). For example, educational or awareness campaign may be employed to flag and correct highly threatening messages coming from close to the location of interest and around key events in order to reduce chaos and uncertainty related to the event. This preliminary study lays the foundation for future studies targeting at uncovering more complex issues.

As a theoretical contribution, we have demonstrated the effect of proximity on threat appeal and sharing behavior. Prior literature has established that threat situation serves as an important antecedent of cyber-rumor sharing (Kwon and Rao 2017). In this paper, we have shown support for our claim that in addition to threat situation, proximity also serves as an important antecedent of cyber-rumor sharing. Proximity is an underlying mechanism that forms the exposure to threat (Kwon et al. 2017), which in turn affects social media users' willingness to share cyber-rumor messages. In this way, proximity can also be considered as one way to collectively manage fear associated with the threat situation.

This study has some limitations. Some of the Twitter messages were in Spanish. We dropped them from the analysis, due to research team's lack of proficiency in Spanish. We coded social distance as a binary variable. A richer scale can be created using individual binary measures for each social circle, such as family, friends, colleagues, etc. Furthermore, the public's characteristics such as age, gender may also influence the relationship between proximity and cyber-rumor sharing[3]. However we do not have such data from Twitter APIs. In order to complete the research further, we plan to investigate if proximity moderates the effect of threat appeals on cyber-rumor sharing. Given the counterintuitive results regarding psychological distance, another potential next step might be to conduct a mediation test (psychological distances - threat appeal - rumor sharing). As a potential future work, we can consider time-varying effect of threat appeal and proximity on cyber-rumor sharing. To elaborate, threat appeal and proximity in the current period may influence cyber-rumor sharing in the next time period. Future studies could also examine generalizability of findings from this one specific event of emerging infectious disease, Zika, to the other events (See footnote 3).

[3] We would like to thank an anonymous reviewer for pointing this out.

Acknowledgements. This research has been funded in part by NSF under grants 1651475. Usual disclaimer applies. The authors would like to thank the reviewers whose comments have greatly improved the paper.

References

Cheng, J.J., Liu, Y., Shen, B., Yuan, W.G.: An epidemic model of rumor diffusion in online social networks. Eur. Phys. J. B **86**(1), 29 (2013)

Folkman, S.: Stress: Appraisal and Coping. Encyclopedia of Behavioral Medicine, pp. 1913–1915. Springer, New York (2013). https://doi.org/10.1007/978-1-4419-1005-9

Goldberg, Y., Levy, O.: Word2vec explained: deriving Mikolov et al.'s negative-sampling word-embedding method. arXiv preprint arXiv:1402.3722 (2014)

Kim, D.J., Song, Y.I., Braynov, S.B., Rao, H.R.: A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. Decis. Support Syst. **40**(2), 143–165 (2005)

Kishore, R., Agrawal, M., Rao, H.R.: Determinants of sourcing during technology growth and maturity: an empirical study of e-commerce sourcing. JMIS **21**(3), 47–82 (2004)

Kwon, K.H., Chadha, M., Pellizzaro, K.: Proximity and terrorism news in social media: a construal-level theoretical approach to networked framing of terrorism in Twitter. Mass Commun. Soc. **20**(6), 869–894 (2017)

Kwon, K.H., Rao, H.R.: Cyber-rumor sharing under a homeland security threat in the context of government Internet surveillance: the case of South-North Korea conflict. Govt. Inf. Q. **34**, 307–316 (2017)

Larson-Hall, J.: Changing the Way We Do Statistics: Hypothesis Testing, Power, Effect Size, and Other Misunderstood Issues. A Guide to Doing Statistics Research Using SPSS. Routledge, New York (2010)

Lee, J., Agrawal, M., Rao, H.R.: Message diffusion through social network service: the case of rumor and non-rumor related tweets during Boston bombing 2013. Inf. Syst. Front. **17**(5), 997–1005 (2015)

Lee, J.K.: Research framework for AIS grand vision of the bright ICT initiative. MISQ **39**(2), iii–xii (2015)

Lee, J.K.: Invited commentary—reflections on ICT-enabled bright society research. Inf. Syst. Res. **27**(1), 1–5 (2016)

Li, J., Vishwanath, A., Rao, H.R.: Retweeting the Fukushima nuclear radiation disaster. Commun. ACM **57**(1), 78–85 (2014)

Liberman, A., Chaiken, S.: Value conflict and thought-induced attitude change. J. Exp. Soc. Psychol. **27**(3), 203–216 (1991)

Marsden, P.V., Campbell, K.E.: Measuring tie strength. Soc. Forces **63**(2), 482–501 (1984)

Nossek, H., Berkowitz, D.: Telling "our" story through news of terrorism: mythical newswork as journalistic practice in crisis. Journalism Stud. **7**(5), 691–707 (2006)

Oh, O., Agrawal, M., Rao, H.R.: Community intelligence and social media services: a rumor theoretic analysis of tweets during social crises. MIS Q. **37**(2), 407–426 (2013)

Osgood, D.W.: Poisson-based regression analysis of aggregate crime rates. J. Quant. Criminol. **16**(1), 21–43 (2000)

Park, I., Sharman, R., Rao, H.R., Upadhyaya, S.: Short term and total life impact analysis of email worms in computer systems. Decis. Support Syst. **43**(3), 827–841 (2007)

Pezzo, M.V., Beckstead, J.W.: A multilevel analysis of rumor transmission: effects of anxiety and belief in two field experiments. Basic Appl. Soc. Psychol. **28**(1), 91–100 (2006)

Rao, H.R.: Behavioral infosec research - towards global trust building. In: Keynote Presented at Workshop on The Bright Internet and Global Trust Building, ICIS 2016, Dublin, Ireland (2016)

Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. J. Psychol. **91** (1), 93–114 (1975)

Shin, J., Jian, L., Driscoll, K., Bar, F.: Political rumoring on Twitter during the 2012 U.S. presidential election: rumor diffusion and correction. New Med. Soc. **19**(8), 1214–1235 (2017)

Snefjella, B., Kuperman, V.: Concreteness and psychological distance in natural language use. Psychol. Sci. **26**(9), 1449–1460 (2015)

Solomon, S., Greenberg, J., Pyszczynski, T.: A terror management theory of social behavior: the psychological functions of self-esteem and cultural worldviews. Adv. Exp. Soc. Psychol. **24**, 93–159 (1991)

Stieglitz, S., Dang-Xuan, L.: Emotions and information diffusion in social media—sentiment of microblogs and sharing behavior. J. Manag. Inf. Syst. **29**(4), 217–248 (2013)

Suh, B., Hong, L., Pirolli, P., Chi, E.H.: Want to be retweeted? Large scale analytics on factors impacting retweet in Twitter network. In: 2010 IEEE Second International Conference on Social Computing (SOCIALCOM), pp. 177–184. IEEE, August 2010

Takayasu, M., Sato, K., Sano, Y., Yamada, K., Miura, W., Takayasu, H.: Rumor diffusion and convergence during the 3.11 earthquake: a Twitter case study. PLoS One **10**(4), e0121443 (2015)

Trilling, D., Tolochko, P., Burscher, B.: From newsworthiness to shareworthiness: how to predict news sharing based on article characteristics. J. Mass Commun. Q. **94**(1), 38–60 (2017)

Trope, Y., Liberman, N.: Construal-level theory of psychological distance. Psychol. Rev. **117**(2), 440 (2010)

Valecha, R., Bachura, E., Chen, R., Rao, H.R.: An exploration of public reaction to the OPM data breach notifications. In: Proceedings of Workshop on E-business (WEB) 2016, Dublin, Ireland (2016)

Valecha, R., Oh, O., Rao, H.R.: An exploration of collaboration over time in collective crisis response during the Haiti 2010 earthquake. In: Proceedings of International Conference on Information Systems (ICIS) 2013, Milan, Italy (2013)

Valecha, R., Volety, T., Vemprala, N., Kwon, H., Rao, H.R.: An Investigation of Cyber-rumor Sharing: The Case of Zika Virus. Workshop on Bright Internet & Global Trust Building, Seoul, Korea (2017)

Volety, T., Valecha, R., Vemprala, N., Kwon, H., Rao, H.R.: Cyber-rumor sharing: the case of Zika virus. In: American Conference on Information Systems, New Orleans, LA (2018)

Webb, H., et al.: Digital wildfires: propagation, verification, regulation, and responsible innovation. ACM TOIS **34**(3), 15 (2016)

Witte, K.: Putting the fear back into fear appeals: the extended parallel process model. Commun. Monogr. **59**(4), 329–349 (1992)

Ye, X., Li, S., Yang, X., Lee, J., Wu, L.: The fear of Ebola: a tale of two cities in China. Big Data Support of Urban Planning and Management. AGIS, pp. 113–132. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-51929-6_7